Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

REPLY COMMENTS OF U S WEST COMMUNICATIONS, INC.

Kathryn Marie Krause
Suite 700
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Attorney for

U S WEST COMMUNICATIONS, INC.

Of Counsel
Laurie J. Bennett

February 10, 1994

TABLE OF CONTENTS

PAGE

SUMMARY

Virtually every commentor in this proceeding supports the basic principle that fraud prevention responsibility should be assigned to the entity(ies) best in a position to prevent the fraud, in the first instance. The lines get drawn with regard to which entity that is.

Both LECs[1] and IXCs generally contend that those entities owning CPE, and having the primary care, custody and control of that equipment, should bear the primary responsibility for fraud "costs" (both prevention and liability). CPE owners (both those owning business CPE and those owning payphone CPE) generally contend otherwise, asserting totally unsubstantiated arguments that carriers are in the best position to prevent fraud; and that fraud "costs" are better spent and absorbed by network providers than by individual customers.

One thing is certain. The parties currently primarily responsible for fraud prevention/liability, i.e., CPE owners, want some relief from that responsibility. They assert specious arguments in support of their positions, including customer ignorance and/or powerlessness, customer diversity, lack of customer financial resources, risk allocation inefficiencies and so on.

Manipulation of existing liability allocation for fraud costs is a fairly profound exercise of legislative authority. It

---

[1]All acronyms used in this Summary are fully defined in the text.

requires an assessment that those costs are currently misallocated (something U S WEST and others dispute) and an interference with existing valid contractual carrier limitations of liability. The Commission should decline to exercise this authority or to mandate the sharing of fraud costs.

The record before the Commission demonstrates that those costs are currently properly allocated: The CPE owner bears primary responsibility for both the costs of fraud prevention and the liability costs. Others support the CPE owner in making sure that owner is aware and intelligent about the problem, about the kind of CPE being purchased, and about services available to that owner to aid in the management of CPE-based fraud.

On the basis of the filed comments, it seems apparent that the Commission need not exercise any kind of formal regulatory authority with regard to telecommunications fraud. Carriers are not using their limitations of liability in an unconscionable manner. Customer education, while currently fairly extensive, appears to still be increasing. Customer warnings are already being conveyed by both LECs (often in a customer service capacity) and CPE vendors. In essence, the paradigm is most economically and technologically efficient as it currently exists. It reflects both the proper legal and market resolution of the problem. It should not be disturbed.

Nor is their any need to disturb the existing prevention/ liability equation with regard to IXCs/OSPs and LECs, insofar as LIDB offerings are concerned. The record demonstrates that the

LECs' LIDBs are responding to market pressures and will be undertaking additional fraud-prevention enhancements during the course of 1994.

The record also demonstrates that the ultimate maximization of LIDB as a fraud-prevention offering depends as much on the actions of the IXCs/OSPs as on the LECs. If IXCs/OSPs do not query LIDB, critical information is not secured by the IXC/OSP and critical input is, concomitantly, not conveyed to the LIDB operator.

Even if the current situation were changed, however, (e.g., some kind of mandatory LIDB query requirement), LECs should not be required to assume greater liability for LIDB errors or validations than they choose to do as a matter of business prerogative and market responsiveness. Assumption of greater LEC liability will only drive the price of the LIDB service up, and will remove incentives from those accepting LEC calling cards to manage the acceptance of those cards in the way most suited to their business operations.

Idiosyncratic IXC/OSP complaints about the operation and performance of LIDB are best resolved between the complaining IXC/OSP and the LEC operator. Systemic problems and overall fraud prevention activities are better coordinated through other fora. The Commission should encourage the continuous engagement of IXCs/OSPs and LECs in periodic fraud reviews and industry consultations. Greater collaboration between LECs and IXCs/OPSs would undoubtedly result in a greater fraud prevention return than mandatory regulatory action.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

REPLY COMMENTS OF U S WEST COMMUNICATIONS, INC.[1]

I. INTRODUCTION

Virtually every commentor in this proceeding[2] supports the basic principle that fraud prevention responsibility should be assigned to the entity(ies) best in a position to prevent the fraud, in the first instance.[3] The lines get drawn with regard to which entity that is.

Both local exchange carriers ("LEC") and interexchange carriers ("IXC") generally contend that those entities owning

---

[1]U S WEST Communications, Inc. ("U S WEST"), is filing these Reply Comments on behalf of ourselves, i.e., the telephone operating company, and with a voice not inconsistent with the interests of our other affiliated companies. Our cellular company, NewVector Group, Inc., is filing Reply Comments on its own behalf through its trade association, the Cellular Telephone Industry Association. Thus, these Reply Comments do not address any aspect of cellular fraud.

[2]A list of commenting parties to which U S WEST cites in this text, with appropriate acronyms, is attached to this filing as Appendix A.

[3]See, e.g., Ad Hoc at 1; AT&T at i, 13; CTIA at 12; Ericsson at 5-6; IPANY at Summary, 1-2, 9-10; NJPA at 1; Pinellas County at 4-5; Sprint at Summary, 8-9; Stop & Shop at Attachment A, 2; TRA at 5; TFS at ii, 2; Vanguard at 2, 5-6; WilTel at 1-2. Compare In the Matter of Policies and Rules Concerning Toll Fraud, CC Docket No. 93-292, Notice of Proposed Rulemaking, FCC 93-496, rel. Dec. 2, 1993 ("NPRM"), ¶ 24.

customer premises equipment ("CPE"), and having the primary care, custody and control of that equipment, should bear the primary responsibility for fraud "costs" -- both those costs associated with fraud prevention and those associated with after-the-fact fraud liability.[4] The CPE owners (both those owning business CPE and those owning payphone CPE) generally contend otherwise, arguing that carriers are in the best position to prevent fraud and that fraud "costs" are better spent and absorbed by network providers than by individual customers.[5] In support of these arguments, commentors urge customer ignorance and/or powerlessness,[6] customer diversity,[7] lack of customer financial resources,[8] risk allocation inefficiencies[9] and so on.

One thing is certain. While much time is spent in this proceeding discussing relative rights/responsibilities of carriers and customers with regard to fraud, SBC is correct that

---

[4]See, e.g., AT&T at 10-11; Cleartel/NorthWest at 8; CompTel at 2; Flex at 2; MCI at ii, 1; NYNEX at Summary, 17-18; Pacific at 8, 11; Sprint at ii-iii, 9-10; Rochester at ii, 2, 5; TCG at 5-6; TRA at 5-6; TFS at ii, 2, 4, 6; USTA at 3; U S WEST at 37-45.

[5]See, e.g., APCC at iii, passim; IPANY at 1-2, 13, 14-15; Leucadia and AIB at 3; MPA at 1-2; NATA at 2, 4, 9; NJPA at 1.

[6]See, e.g., APCC at 1-2, 19; NATA at 8; Pinellas County at 3, 4, 8; RAK at 3.

[7]See, e.g., NATA at 6 (customers do not purchase all equipment from the same source and any one of the discrete pieces of equipment can be network "points of entry"); Pinellas County at 2-5, 7-8; TCA at 7.

[8]See, e.g., APCC at 2; NATA at 9; Pinellas County at 4; TCA at 9.

[9]See, e.g., APCC at 2, 6, 9-10, 11; ARINC at 3; NATA at 7.

the fundamental issue in this proceeding is who picks up the tab for fraud costs -- both the costs of prevention and the after-the-fact liability costs and whether those costs should be shared.[10] The current responsible parties, i.e., CPE owners, want some relief from that responsibility, and assert specious arguments in support of their position that they deserve relief.

Manipulation of existing liability allocation for fraud costs is a fairly profound exercise of legislative authority. It requires an assessment that those costs are currently misallocated (something U S WEST and others dispute) and an interference with existing valid contractual carrier limitations of liability. The Federal Communications Commission ("Commission") should decline to exercise this authority or to mandate the sharing of fraud costs. The record before the Commission demonstrates that those costs are currently properly allocated: The CPE owner bears primary responsibility for both the costs of prevention and the liability costs. Others support the CPE owner in making sure that owner is aware and intelligent about the problem, about the kind of CPE being purchased, and about services available to that owner to aid in the management of CPE-based fraud. In essence, the paradigm is most economically and technologically efficient as it currently

---

[10] See SBC at 3 (quoting from the NPRM ¶ 25, "whether to apportion the cost of CPE-based fraud").

exists. It reflects both the proper legal and market resolution of the problem.[11] It should not be disturbed.

Nor does the record support a holding that LEC liability for fraud losses needs to be increased to spur LECs on to greater or more earnest fraud prevention activities. The record demonstrates that LECs are currently vigorously engaged in various telecommunications fraud prevention activities, ranging from customer education to providing network access restrictions and network screening services. The engagement of these providers demonstrates an ongoing commitment of money and personnel to fraud prevention. It also patently demonstrates the logical flaw in any argument suggesting that LEC interest in fraud prevention can be generated only through manipulation of LECs' ultimate financial liability for telecommunications fraud that does occur.

On the basis of the filed comments, it seems apparent that the Commission need not exercise any kind of formal regulatory authority with regard to telecommunications fraud. Customer education, while currently fairly extensive, appears to still be increasing. Customer warnings are already being conveyed by both LECs (often in a customer service capacity) and CPE vendors. Payphone provider liability appears to be fairly well aligned with owners' self-help purchase of LEC blocking/screening service.

---

[11] See WilTel at 5-7.

IXCs are offering network monitoring services to aid their customers in managing those customers' fraud prevention responsibilities. In those circumstances where a CPE owner fails, despite its best efforts, to ascertain the occurrence of fraudulent calling, such network monitoring services operate as a second-line, or complementary, defense to the problem.[12] Additionally, certain IXC "fraud insurance" offerings are structured in such a way that a CPE owner who does in fact undertake a "best efforts" approach to fraud prevention, can -- in return -- assure itself of capped liability for fraud which occurs.

LECs' Line Information Database ("LIDB") services are being enhanced with greater administrative and substantive capabilities, such that more fraud prevention capabilities will be available before the end of the year. Additionally, audit trails will become available that will make assessing LIDB query access easier. In light of all of this information, it appears that the marketplace is in fact responding quite adequately to the matter of fraud awareness and prevention -- matters that should constitute the Commission's focal point in this proceeding.[13]

In light of the record, there is little to support Commission intervention in the manner in which carriers

---

[12]See TeleDesign at 2.

[13]See, e.g., Cleartel/NorthWest at 2-3, 10; CompTel at 1; LinkUSA at 3; NTCA at 1; Pacific at 3; USIN at 2, 3; USTA at 1-2, 5-6; Vanguard at 2; WilTel at 5-7.

ultimately respond to perpetrated fraud. Carriers are not using their limitations of liability in an unconscionable manner, and nothing in the record would support such a finding. Rather, they are using them as other commercial suppliers do: to avoid liability for mistakes and for negligence, as such liability is not included in their product offerings. While certain commentors complain about the use of such provisions, and others assert that such provisions should not be permitted in various factual scenarios, no commentor convincingly demonstrates that such provisions are unlawful or are contrary to either commercial or telecommunications public policy.

In the absence of any need for formal Commission intervention, U S WEST encourages the Commission to lend the power of its office to fraud prevention in a more facilitating capacity.[14] While no mandatory or prescriptive Commission action need be taken with regard to existing carrier behavior, it appears that there still remains some industry/customer contention that should (and could) be converted to closer cooperation. And, it is obvious that more fraud prevention work is on the horizon, particularly with the growth of Personal Communications Services ("PCS") and other wireless services.[15] This kind of ongoing bridge-building and investigative type of work can best be done in an industry organization focused on the technologies and politics of fraud prevention and liability

---

[14]See SNET at 2.

[15]See, e.g., AT&T at 36; Bell Atlantic at 1.

allocation. The Commission should assure the existence of such an organization.

II. THE CPE OWNER (WHETHER BUSINESS OWNER OR PAYPHONE PROVIDER) SHOULD BE THE ENTITY PRIMARILY RESPONSIBLE FOR FRAUD COSTS, BOTH PREVENTION AND LIABILITY -- IF THE BUSINESS CANNOT BEAR THOSE COSTS, THE BUSINESS SHOULD NOT BE IN BUSINESS

A. The Network is Not the Best Place to Prevent Fraud

The Commission must decide, as a preliminary matter, whether -- as a matter of formal regulatory policy making -- fraud costs should be shared, or whether they are currently allocated quite appropriately. The importance of this predicate decision cannot be underestimated, because from it all other decisions in this proceeding flow logically, e.g., whether further warnings are necessary, whether limitations of liability need to be changed.

A number of commentors appropriately cite to the Commission's observation that intelligence from the network has migrated out into equipment located on customers' premises.[16] With that migration, the customer has gained a benefit (i.e., increased intelligence, customization, and flexibility) and has been burdened with a cost (i.e., fraud). As a result of that migration, common carriers lost something as well (i.e., total control, on an end-to-end basis, of the customers' calling behavior; revenues from network-based services that are now performed in CPE). Having lost control of the basic call set-up

---

[16]See GTE at 2; AT&T at 10 n.9; TFS at 4; WilTel at 2, 9 (all citing to the NPRM ¶ 3).

process, they should not be expected -- at this point in time -- to absorb the costs of fraudulent call set ups.

It is not enough to argue, as some do, that customers lack the kind of sophistication necessary to protect themselves against fraud,[17] or that they often employ a telecommunications system tying together various constituent parts,[18] or that certain peripheral telecommunications markets or other market segments are not capable of absorbing any greater fraud costs.[19] If the costs of fraud are most appropriately allocated to the CPE owner, then that owner has some options: get smarter, learn more, buy additional equipment, get out of the business.[20] One option the CPE owner does not have is to ask someone else to "share" in that properly allocated cost.

The request for "sharing" is particularly inappropriate when it is shrouded in the argument that some other entity actually should be the primary responsible party for fraud: i.e., the network providers. While carriers are clearly demonstrating an increased willingness to meet a market demand for customer education and network aids to complement existing built-in CPE

---

[17]See, e.g., APCC at 1-2, 18-19; NATA at 8; Pinellas County at 3-4, 8.

[18]See, e.g., NATA at 6-7. Compare AT&T at 11 (this factor would, in fact, argue for primary responsibility of the CPE owner to protect against fraud, not against it).

[19]See, e.g., Ericsson at 3 (regarding the CPE market); APCC at 1-2 (regarding the payphone market); Pinellas County at 4 (small businesses); TRA at 4-5 (the switchless resale market).

[20]Compare TeleDesign at 1.

fraud prevention capabilities, requiring that the network operate as a kind of Maginot line with regard to fraud prevention with respect to each and every end user on the public network is, as GTE argues, both inefficient and unwarranted.[21]

The "network first" argument, while repeatedly made, never really is analyzed. The proposition is asserted in one of two ways: 1) network providers should be primarily responsible for fraud, and therefore they should be required to act more aggressively with respect to network monitoring (in essence, a philosophical or ideological argument with specific factual consequences);[22] or 2) network providers are technically most capable of preventing fraud in the network, as a result of the ubiquitous, common reach of the network as opposed to the idiosyncracies of CPE.[23] Neither of these arguments is correct.

As we have demonstrated above, there is no sound philosophical or ideological reason to impose on carriers the primary responsibility for fraud control -- either its prevention or its financial consequences. Thus, the first argument fails as a matter of philosophy or logic.

---

[21]See GTE at i, 4-6.

[22]See, e.g., API at 4-6; ISLUA at 2-3; NJPA at 1-2; UTC at 5. A subsidiary argument here is that it is network services that are being stolen when fraud occurs and so the prevention should be directed to the services, not the access devices. See, e.g., APCC at 11; NATA at 4; User Parties at 8 n.16.

[23]See, e.g., Ad Hoc at 3; APCC at 9-10, 11; ARINC at 3; MPA at 2; NJPA at 1; Stop & Shop at Attachment A, 1; User Parties at 5.

With its demise, the suggestion that increased network monitoring be required as a part of existing common carriage obligations also fails. It is not true as a matter of physics or engineering (as well as of public policy theory) that the network is the best (or the primary) place to guard against fraudulent conduct.[24] All carriers, to be sure, have existing network monitoring equipment in place. The purpose of that equipment is to manage the network, both its overall performance and its security. Network monitoring is done in gross, with respect to the overall operation of the network as a network -- not as an amalgam of hundreds of individual lines or trunks.[25] While, in

---

[24]See Xiox at 3 (network-based security solutions may be more expensive and less flexible/controllable than other solutions).

[25]See MCI at 8 (noting the limited capacity of carrier network monitoring to protect against fraud, especially when a customer's traffic traverses more than one network); AT&T at 10-11 (to the same effect). Compare User Parties' argument that the network providers "alone possess contemporaneous information regarding traffic patterns and call volumes." User Parties at 5. This may be true, but not with a view to changing/correcting such activity on discrete lines or trunks, unless the traffic patterns or call volumes are interfering with overall network performance.

API observes that "the major carriers possess the ability to detect ongoing incidents of fraud on a real-time basis," and goes on to discuss how it is obvious that some time needs to pass in a predetection stage before a carrier could be held to have knowledge of fraud. See API at 8 n.8. Having an "ability to detect" is different from attending to the detection of fraud. A carrier monitoring its network might determine, at the end of a specific time period and as a result of its own network monitoring responsibilities, that something looked awry. But it would not have been looking for something awry from a discrete customer perspective unless someone had told the provider to do so. The differences in the phenomena are akin to a person having the ability to find money if they are walking down the street looking at the ground checking for dangerous holes or disruptions

(continued...)

the course of that monitoring, on occasion a problem will (might) be spotted with respect to an individual line or trunk, that discovery is secondary to the purpose of the monitoring.

To convert current network monitoring activities into more discrete line/trunk monitoring would involve substantial costs -- costs that should appropriately be recovered from those who need or desire such monitoring. For that reason, among others, carriers that devise such additional, new monitoring capabilities will generally be inclined to charge for them. In substance, these kinds of monitoring capabilities are "dedicated" to a purpose quite different and apart from overall network performance and reliability.

As SBC asserted, the argument is akin to asserting that interstate highway providers are primarily responsibility for car thefts that occur on the highway.[26] While both kind of providers will take various steps to provide the safest highway possible (e.g., posted speed limit signs, radar guns, patrol

---

[25](...continued)
and a person out looking for money on the same street, maybe even with a metal detector. In the first instance, finding money is a result of the fact that the person happened to be on a street where there was money, and happened to be looking down, where the money was. In the second instance, finding the money was the objective of the task, and the objective was enhanced by additional tools of the endeavor. They are very different activities, stemming from different purposes. See AT&T at 13-14; Sprint at ii, 10; LinkUSA at 2 (the creation of "fraud monitoring" "system[s] requires intensive development"), 4.

[26]See SBC at 3. Or, as Pacific put it, the argument is akin to "holding a taxi driver who takes a customer to the airport responsible when that customer highjacks an airplane." Pacific at 10.

cars; customer education and warnings, internal monitoring devices for telecommunications traffic aberrations, network attendants, etc.), liability for losses resulting from individual decisions (e.g., the kind of theft protection mechanisms built into the car -- a simple door lock (if any lock at all) to a state-of-the-art anti-theft device) and miscreant acts of criminals cannot, under any theory of causation, be allocated to the provider of the highway.[27]

Skipping over the entire problem of causation, those who espouse that carriers assume a larger portion of the fraud tab assert that you can get more fraud prevention "'bang for the buck'"[28] from the network than you can from the multiple CPE

---

[27]See SBC at i, 3. This is true despite the fact that it would be possible for the transport provider to increase the security of the system, e.g., to place cameras along the highway, to add additional highway patrol cars, to close the highway in evening hours; to increase monitoring in the telecommunications network.

[28]See, e.g., NATA at 7. The reasons NATA espouses for why manufacturers should have only limited liability for toll fraud, are equally applicable to network providers. For example, NATA argues that manufacturers are not in a position to control the placement of CPE "in the field." See id. The same is true of network providers. It argues that manufacturers are not in a position to control telecommunications systems composed of various constituent elements by different entities, any of which can be the first "'point of entry' that is implicated in toll fraud." See id. The same is true of network providers. Finally, NATA argues that manufacturers have "virtually no control over whether [CPE] is operated in accordance with instructions" or "that the equipment is monitored for unusual calling patterns." See id. (emphasis added). Neither does the network provider. Yet, rather than assuming any additional prophylactic obligations be borne by manufacturers (such as on-site monitoring, etc.), NATA argues that network providers are in the best position to protect against fraud. The logical fallacy of the argument is apparent when an analogy such as the one above is considered.

points of entry. However, this is never demonstrated to be true. And, it is not intuitive. To use SBC's analogy again, a society could protect against car theft on interstate highways by developing and deploying a highway model that does not currently exist. For example, all users of the highway could be subject to a pre-access security check, and those with clean records could be provided an identification card allowing them highway access. A stop-point could be created to determine a driver's right to pass. The highway system administrator could also place a patrol officer at every xx feet on the highway, assuring that no car is left with a problem that might later allow the vehicle to be stolen. Alternatively, a society can reasonably protect against car theft on the highway by expecting that persons who have to vacate their cars will lock their cars and hope for the best. The better lock the person has, the more likely their car will be there in the morning, if a potential entry is attempted. Similarly, fraud could be protected against in the telecommunications network by creating a different kind of network (e.g., customer calling caps either by traffic or dollar volume, calls permitted only to certain customer-designated NPAs), or fraud can be protected against by asking that entrants secure their access vehicles, as they deem most appropriate. The better the security, the less likelihood of fraud. But, the choice remains that of the customer. The customer decides the

level of security desirable, based on its own cost/benefit analysis.[29]

Those who want increased sharing in fraud costs by carriers also assert that network providers have more resources than CPE owners, including payphone providers,[30] the implication being that such providers should "share" the costs because they can.[31] In essence, those who advocate a "network first" model of fraud prevention or who seek to insulate CPE owners from fraud based on some ill-defined criteria of CPE owner "reasonable actions" taken, may be well intentioned, but the logic is just plain wrong. As GTE said, such a policy "merely reassigns liability for fraud [and] mask[s] its presence[.]"[32]

---

[29]See LinkUSA at 4; WilTel at 5-7.

[30]See, e.g., APCC at 2; NATA at 9.

[31]See, e.g., ISLUA at 4. Compare NPRM ¶ 29, which may have given some impetus to such an argument by suggesting that entities other than the CPE owner might be "better able to absorb the costs of fraud than payphone providers." The matter should not be who can best absorb the loss, but whether the loss is properly allocated, in the first instance. See AT&T at 18; GTE at 12.

[32]GTE at 11. Compare id. at 2. Indeed, it is important to note that the "evidence" submitted on the "success" of the Florida payphone model (see NPRM ¶ 31, requesting evidence of success) is made up solely of the fact that no administrative filings or complaints have been proffered since its adoption. See FPSC at 3, emphasis added ("Prior to the implementation of the revised rules, the FPSC had several cases pending before the Commission regarding fraudulent calls billed to pay telephones. Since implementation of these rules, there have been no complaints, problems or disputes brought before the Commission."). Compare FPTA at 1-2, 7. Hardly a stellar endorsement. A fairly limited problem (i.e., "several cases") resulted in a major change in risk/cost allocation. The lack of current Commission involvement demonstrates nothing about the

(continued...)

B. CPE Owners Must Exert Their "Best Efforts," Not Just Reasonable Efforts, to Protect Themselves Against Toll Fraud

If the CPE owner is the primary entity responsible for fraud committed over its CPE (as has been the case in the past), then certain propositions follow: That owner must exert its best efforts, not just reasonable efforts, to protect itself against fraud. In many cases, if best efforts were exerted, the potential for fraud would be greatly diminished.

APCC,[33] as well as other payphone and non-payphone CPE owners,[34] argue that CPE owners/COCOT providers should be completely "exempt" or "insulated" from fraud liability once they have exerted "reasonable" efforts to protect themselves against fraud. "Reasonable efforts" would include the purchase of LEC-offered blocking and screening services and maybe more, but maybe nothing.[35]

---

[32](...continued)
sagacity -- either logically, economically or from a market or public policy perspective -- of the model. It simply demonstrates that CPE owners who do not have to contend with the consequences of their business entry or purchase decisions are generally happy about it. That does not make it good policy.

[33]See APCC at ii, 6, 8, 10, 14, 19-20.

[34]See, e.g., ARINC at 3; ICA at 2-3; IPANY at 7, 10; MPA at 2; NJPA at 1-2; SCOIR at 5; UTC at 6.

[35]Part of the difficulty in analyzing this argument is that some commentors urge that if the COCOT provider has purchased LEC-offered blocking/screening services, then they would have no liability (see, e.g., IPANY at 9 (blocking/screening an no PIC option); SCOIR at 6); others argue that the purchase of such services would certainly constitute reasonable efforts, but there
(continued...)

The Commission should reject this position. If CPE owners are required to exert only reasonable efforts, someone is going to be responsible for exerting "best efforts."[36] A "best effort" obligation should reside with CPE owners, not network providers.[37] The CPE owner makes the purchase decision. The

---

[35](...continued)
may be other actions required as well, and they ask the Commission to specifically define what those other efforts might be (see, e.g., APCC at ii, 4, 10, 14, 23; MPA at 2; NJPA at 2; NATA at 2; 5-6). Still others argue that while CPE owners/COCOT providers might have a theoretical obligation to exert reasonable efforts to prevent against fraud, if carriers do not live up to their respective obligations for fraud prevention (as defined by the commentors), then the CPE owner/COCOT provider should be relieved of liability even if it took no preventive action. See APCC at 22; NATA at 16. While variations on a theme, the "reasonable" conduct expected of the CPE owner/COCOT provider becomes increasingly diffuse.

[36]If all entities involved in fraud prevention exerted reasonable efforts, there would be a substantial amount of fraud which would occur, but not necessarily the result of any entity's negligence. Virtually all commenting CPE owners/COCOT providers would have that "residual" liability reside with the network providers. That is, while seeking fault-based liability for themselves, they do not necessarily advocate a similar standard for the network providers. U S WEST would support the Pacific theory that, absent negligence by the carrier (and gross negligence at that, pursuant to valid LEC limitations of liability) that "the party who would normally reap the business reward should shoulder most of the liability." Pacific at iv, 9-10, 14. See also Sprint at 10.

[37]Stated another way, CPE owners do not exercise reasonable efforts to prevent payphone fraud solely by purchasing LEC-offered blocking and screening devices, or taking other such "first line" defenses. More is often required. Compare AT&T at 11 n.10 ("In AT&T's experience, occurrences of fraud have never required a customer to completely discard its existing CPE. In nearly all cases, the fraud can be controlled by making relatively simply changes in the existing equipment -- or simply by acting more prudently in assigning and monitoring the use of access codes."); Bell Atlantic at 6 ("[m]ost payphone providers do not use all the capabilities available to them"); Ericsson at 3, emphasis added (CPE fraud "can be effectively controlled if
(continued...)

COCOT provider makes the placement decision.[38] Inherent in both decisions are exercises in choice, reflecting a balancing between preventing fraud up front (i.e., by expending resources on preventive intelligence or physical monitoring of equipment) and the possibility that fraud will occur, resulting in after-the-

---

[37](...continued)
parties that purchase [CPE] use all reasonable means to protect against fraud."); MCI at 10-11 (a reprogramming of payphone CPE might be required, the establishment of "cuckoo tones" might be needed or the location placement might need to be changed); RAK at 4 ("There are a number of possible software steps which can be taken in the system either at the discretion of the installation team or the direction of the customer. It is too easy to simply ignore these possibilities out of a desire to minimize the installation labor (those associated with a new system or software upgrade/changes) or out of ignorance."). And see LinkUSA at 3; PaPUC at 10-11; Sprint at iii, 12; TeleDesign at Summary. See also note 38, infra.

[38]APCC makes the woeful claim that COCOT providers "make their telephones available to all members of the public and have no significant control over who has access to their payphones" (APCC at 1); and that such providers "cannot control access to their payphones as other subscribers can." Id. at 2. This "poor me" approach to advocacy is ineffective. It claims both too much and too little.

COCOT providers are not generally held to any kind of public utility obligation with regard to their business operations and are free to place their phones anywhere they wish. The environmental decision is totally within the control of the payphone provider. See SBC at 7-8; MCI at 3; NYNEX at 20; Sprint at 12. Private payphone providers have made an affirmative business decision to be in the COCOT business, an admittedly risky business (especially given long-standing law on the responsibility of CPE owners for calls -- both legitimate and illegitimate -- placed from their equipment), and have considerable choice/control over the environment in which they place their phones, albeit not as much control as if they chose not to go into the business and sought to maintain control only over their internal home or business telephone. It is simply untrue, as APCC alleges, that COCOT providers are "least able to take effective measures to prevent fraud." APCC at 7. They are in the best position, although taking the responsibility seriously might well change the cost configuration of the business they chose to enter.

fact losses.[39] While the CPE owner can enlist the support of others in aid of its purchase or placement decision, it cannot demand it, as a matter of right.

This is especially true since the CPE owners demand support from network suppliers who have absolutely no control over either the CPE functionalities (either those which are activated or deactivated), the security of the premises, or the education or motivation of the owner to protect against fraud.[40] A network provider should not be expected to assume responsibility for fraud caused by or facilitated by equipment over which the carrier has no control and regarding which it has no risk management authority. As CompTel has stated, "The Commission cannot reasonably impose any [CPE] fraud liability upon [carriers] without giving [carriers] the rights necessary to manage their risks prudently."[41] Such carrier "rights" would include CPE purchase decisions, security activation features/functionalities, and refusal to serve.[42] Obviously, CPE owners would not be very willing to turn over this kind of "risk management" control to a carrier,[43] despite the fact that

---

[39]See, e.g., LinkUSA at 4; WilTel at 5-7.

[40]See CompTel at 2; AT&T at 11; MCI at 3, 5, 7.

[41]CompTel at 4.

[42]See id. And see Sprint at 10.

[43]Indeed, a CPE owner will not generally be agreeable to "negotiating" such prerogatives/control with a network provider, absent some strong external motivation to do so -- such as undesired liability. Compare Ad Hoc at 3-4 n.2.

they want carriers to assume responsibility for a large portion of the risk.

III. THE RECORD DEMONSTRATES NO NEED FOR FORMAL COMMISSION ACTION WITH REGARD TO CARRIER FRAUD PREVENTION ACTIVITIES

A. The Record Demonstrates that LECs and IXCs Both Currently Engage in Extensive Customer Education, Including Warning About the Dangers of Telecommunications Fraud -- No Further Carrier Actions Should be Mandated

This proceeding was launched in 1993 -- not five years earlier. It is obvious that in the past five years customers have become very aware of fraud potentialities, as SBC observes.[44] Lack of customer awareness is not the problem, although customer hubris might be.[45]

The record is replete with carrier demonstrations of the scope and nature of their current, and ongoing, customer education campaigns.[46] Over the past five years, LECs and IXCs alike have developed education materials for their range of customers calculated to inform those customers about the risks associated with improper use of telecommunications services and

---

[44] See SBC at 2-3. See also AT&T at 8-9, 13; CompTel at 5; NTCA at 2 n.2; Sprint at 6 & n.3; WilTel at 6-7.

[45] See, e.g., RAK at 3; Xiox at 3;

[46] The provided information covers fraud prevention materials associated with calling cards, Private Branch Exchanges ("PBX"), Centrex services, 800 and 900 calling and payphones.